RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: SBV-M02

Better Tabletop Exercises: Bringing Operations to the Table

Bryson Bort
CEO SCYTHE

Trey Bilbrey
Lead Adversarial Engineer
SCYTHE

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

@brysonbort

SCYTHE

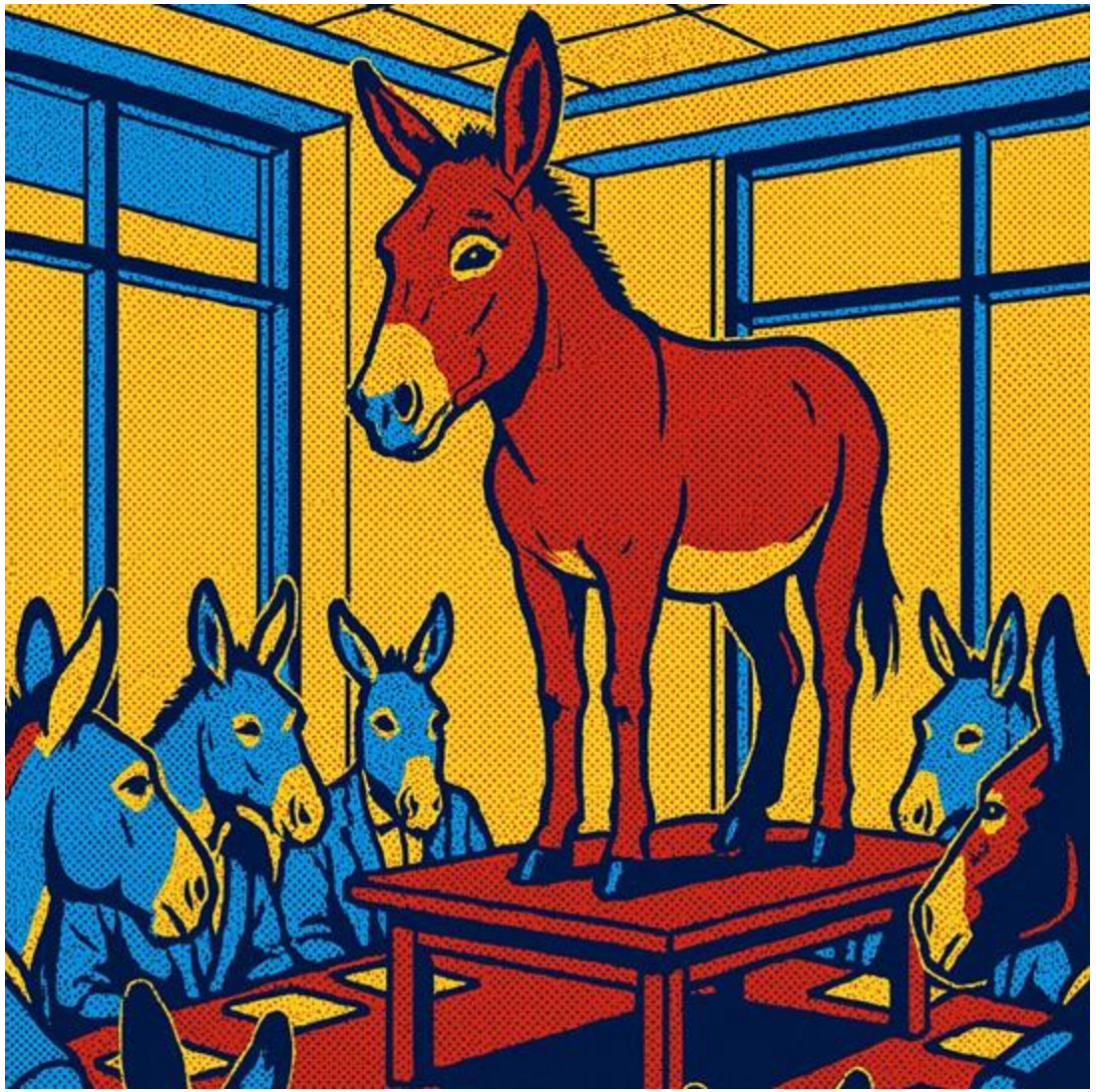
ICS

GRIMM

> Who Am I ?

- George “Trey” Bilbrey @tcraf7
- Professional Services Lead @ SCYTHE
- Co-Founder and community leader for NEON TEMPLE
- Certs and things..

Who Has Been Through A TTX Before?



Current Landscape

Weighed & Measured

There is no immediate **validation** of whether these plans actually work under real-world conditions.

Leadership and security teams **assume** security controls, playbooks, and procedures will work as expected

…but assumptions can be **dangerous**.

Assumptions

- Responses tend to be **hypothetical**:
  - “We would follow our incident response plan.”
  - “We have a policy for handling ransomware.”
  - “Our team knows what to do in this scenario.”

- Tool capabilities
  - “Our EDR would block that”
  - “We have PowerShell locked down”

- Common knowledge to one team member is known by all..

CTEM

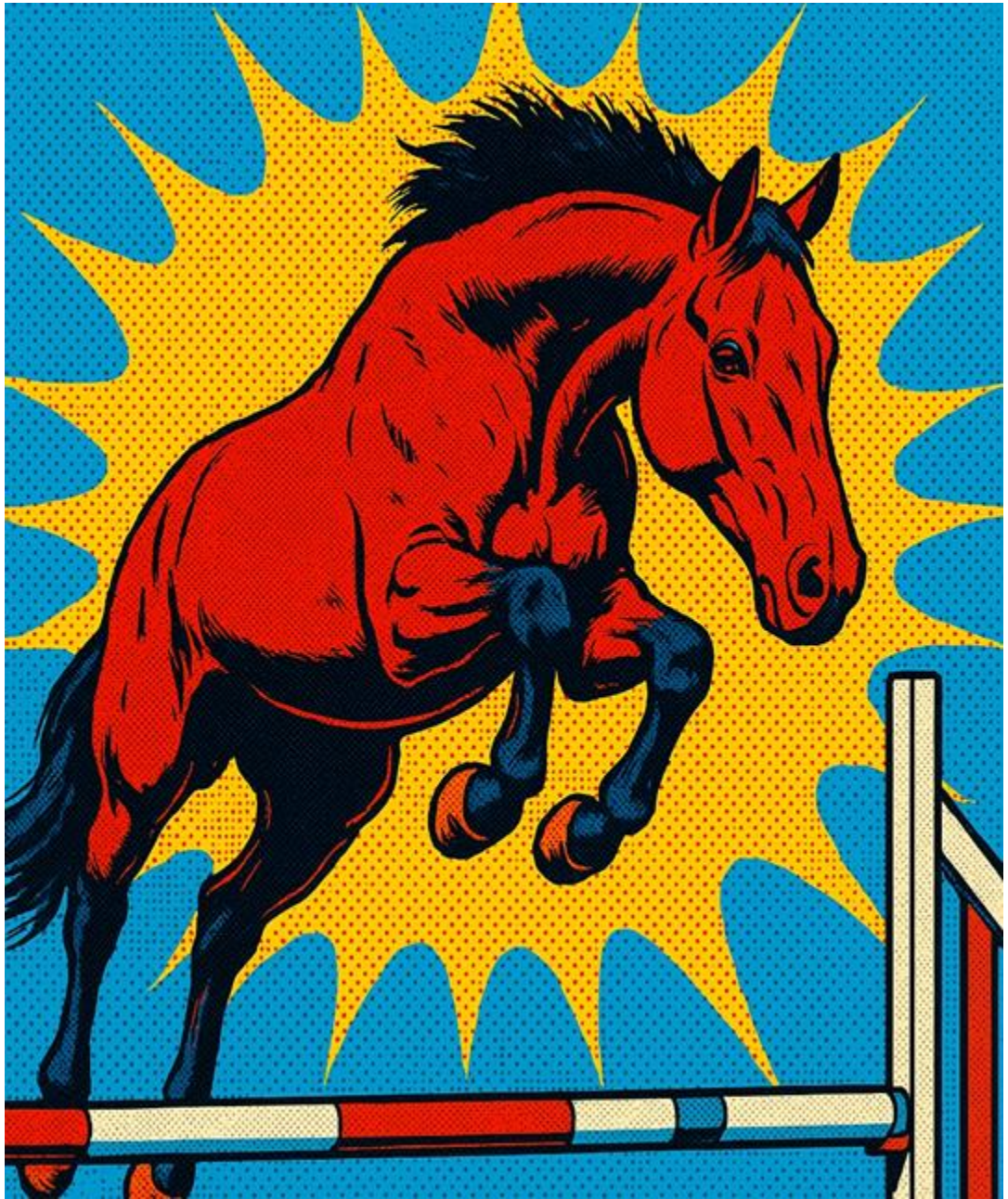
5 Steps in the Cycle of Continuous Threat Exposure Management
5
Mobilization
1
Scoping
Action
Diagnose
4
Validation
2
Discovery
3
Prioritization
gartner.com
Source: Gartner
© 2023 Gartner, Inc. All rights reserved. CM_GTS_2477201
Gartner

RSAC 2025 Conference

Many Voices.
One Community.

What If We Can Do Better?

A Better Way



Compliance

- Existential foundation of business ops

- 2 kinds of leadership, Those that care about security…
  and those that don't.

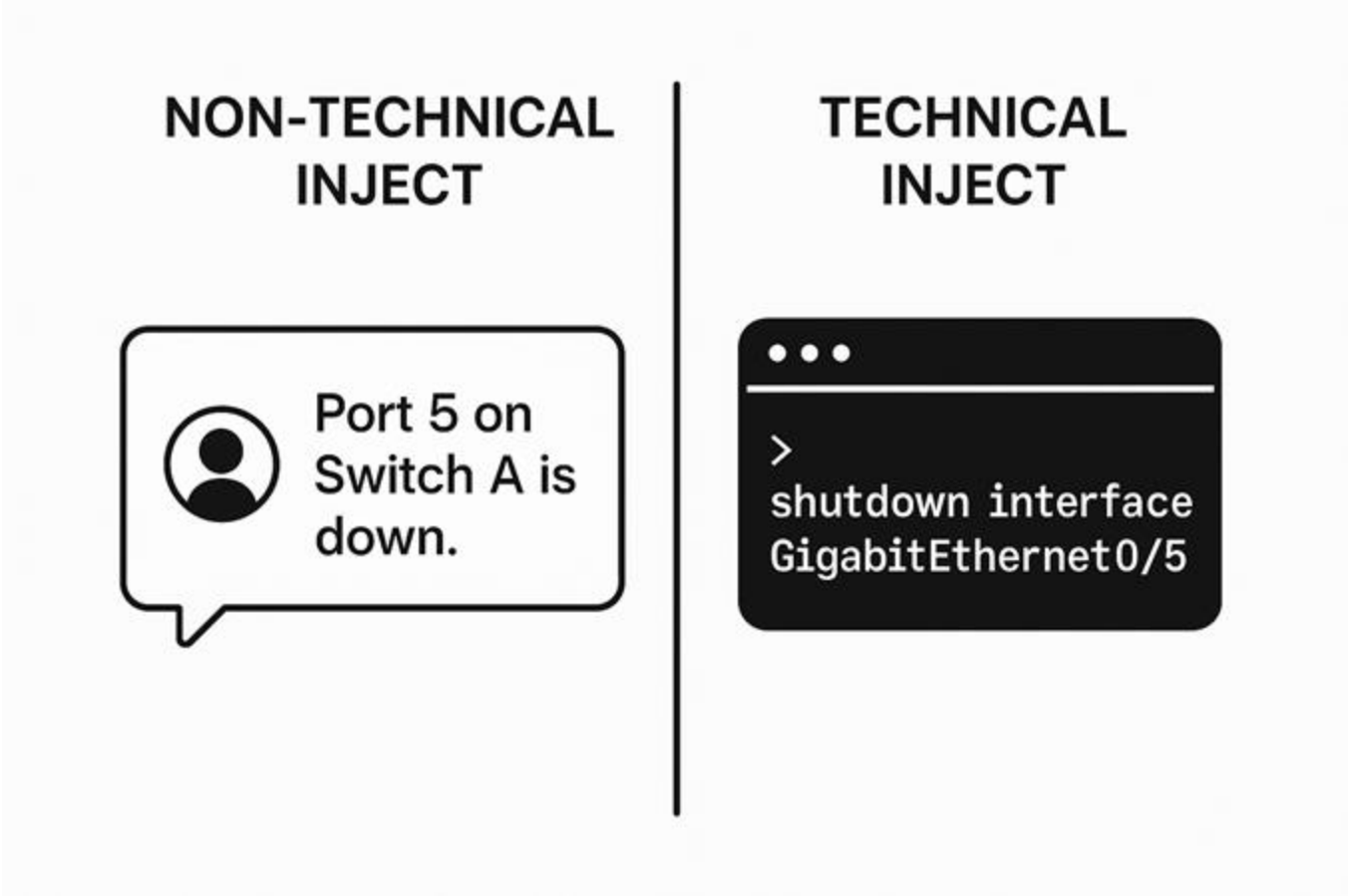
Changing Our Stars

Moving from a compliance-driven approach to a continuous improvement model

Criteria	CTEM	Compliance-Based Security
Effectiveness	**High** Targets real threats with continuous validation.	**Moderate** Ensures baseline controls are met.
Risk Reduction	**Moderate / Proactive** Reduces risk based on threat exposure exploitability.	**Low / Reactive** Analyzes risk periodically.
Attack Prevention	**High / Advanced** Identifies and mitigates before exploitation	**Low / Basic** May miss evolving or new threats.

Reinforcing The Scenario

Incorporating a real-world attack simulation into TTXs allows teams to practice incident response under realistic conditions.



RSAC 2025 Conference

Many Voices.
One Community.

How We Did It

How We Did It

- Defined Scope for testing that includes **EVERYONE**
- Crafted a narrative to include:
  - hands on participation via PTE injects
  - non-technical validation injects based on scope
- Add injects where the team has to demonstrate proficiency, not just lip service
  - “Show me where its documented”
  - “Did you get alerts on X behavior?”

Defining our Scope

- What is the goal of the assessment?
- What do we have access to?
  - Assets
  - Knowledge
  - Personnel

What other teams can we involve? (legal, PAO, etc.)

Defining our Scope

Scenario #1 - Outline

1. **White card** : device plugged in > supply chain compromise
2. **Part WC / part technical** : vuln service used for access > initial foothold/persistence put in place
3. **Technical** : ingress tool transfer > download energyspark_upgrade.exe
4. **Technical**: host recon > host network settings
5. **Technical** : Ping Sweep > additional host discovery
6. **Technical / possible WC** : Lateral movement via Emergency Response Auditor.
7. **Non-Technical** : Identify C2 > build threat picture > Determine exposure
8. **Non-Technical** : endpoint containment > IR wrap-up

Kicking Things Off

Scenario #1 - Inject 1

- The Network Team reports that a network switch in a field office is reporting a number of port shutdown events.
- Further investigation by the network team identifies the same MAC address connecting to the switch on multiple ports triggering the port security shutdown.
- The Network Team reports this to the SOC as a suspicious event.

```
(4096 bytes):

%PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/1, putting Fa0/1 in e
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC .
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state n
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
```

Blending Non-technical & Technical Injects

Request (3/10/2025, 1:48:10 PM)

```
--cmd (New-LocalUser -Name "barnesjb" -Password (ConvertTo-SecureString 'P@ssW0rd11!!' -AsPlainText -Force) -
FullName "James Bucky Barnes" -Description "The Winter Soldier's Admin Account")
```

Response (3/10/2025, 1:48:13 PM)

```
Name     Enabled Description
----     ------- -----------
barnesjb True    The Winter Soldier's Admin Account
```

```
--cmd (Add-LocalGroupMember -Group "Administrators" -Member "barnesjb")
```

Crafting A Story

- Telling a story will drive a great exercise.

Practice Briefing

- The engagements also include dry runs where teams would brief the exercise coordinators (or org leadership).
  - What do they know so far?
  - What is your next step?
  - Should you escalate?
  - Who else should be involved?

Proof Or It Didn't happen

- When policy or SoP would dictate how an inject was handled:
  - Can they point to the policy?
  - Do they understand it and where to find it?
  - Do their actions match what is documented?

Documentation Is Key

What's In It For You?

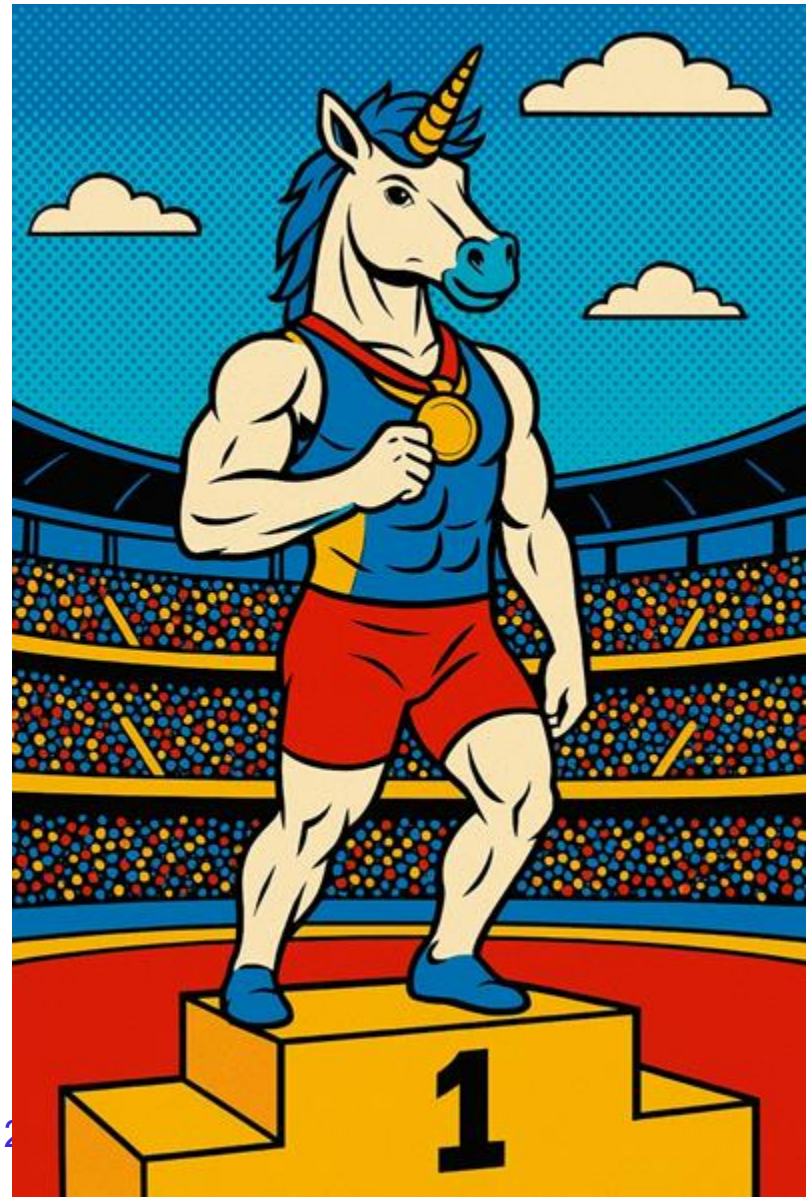
Continuous Refinement of your security posture:

- Personnel
  - Continuous training and adaptation to the threats you face
- Processes
  - Streamlined procedures and understanding of roles
- Tooling
  - Reduced noise and improved response times

Offensive Maturity Model

How To Apply This Approach

- Start with Purple Teaming
- Integrate PTEs with TTXs
- Leverage Data to Drive Decisions
- Make Security a Continuous Process



RSAC 2025 Conference

Questions?